Spring Vale Primary School
eSafety Policy 2023-24

Together Everyone Achieving More	**Together** with friends, families and community we care for ourselves, each other, our school and our world. **Everyone** has access to a broad, balanced and stimulating curriculum, whatever their gender, race, ethnicity or ability. **Achieving** our best is what we aim for every day we come to school. **More** independence makes better learners and helps us to become good citizens.

Contents

- Social Media - Protecting Professional Identity
- Communications
- User Actions - unsuitable / inappropriate activities
- Responding to incidents of misuse
- Security and Privacy
- Responding to incidents of misuse
- Security and Privacy
- Internet Safety
- Preventing Extremism and Radicalisation
- School Ethos and Practice
- Filtering and Monitoring

Development / Monitoring / Review of this Policy

This e-safety policy has been developed by a working group made up of:

- *Chris Blunt / Katie Kelly*
- *Aneil Andreas*
- *Staff – including Teachers, Support Staff, Technical staff*
- *Matt West. Chair of Governors*

Consultation with the whole school community has taken place through a range of formal and informal meetings.

Schedule for Development / Monitoring / Review

This e-safety policy was approved by the Governing Body on:	
The implementation of this e-safety policy will be monitored by the:	E-Safety Coordinator, Senior Leadership Team,
Monitoring will take place at regular intervals:	Once a year
The Governing Body will receive a report on the implementation of the e-safety policy generated by the monitoring group (which will include anonymous details of e-safety incidents) at regular intervals:	Once a year
The E-Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	July 2024
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	LA ICT Manager, LA Safeguarding Officer, Police

The school will monitor the impact of the policy using:

- Logs of reported incidents
- Monitoring logs of internet activity (including sites visited)

- Internal monitoring data for network activity
- Surveys / questionnaires of
  - students / pupils
  - parents / carers
  - staff

Scope of the Policy

This policy applies to all members of the school (including staff, pupils, student teachers, volunteers, parents / carers, all visitors and community users) who have access to and are users of school ICT systems, both in and out of the school.

The school is aware that the Internet is an integral part of 21st Century learning and as such the school has a duty to provide its students with quality Internet access as part of their learning experience. Alongside this, there are provisions which need to be adhered to in order to ensure the safety of our students when online.

Access to computers, devices and the internet is a privilege and not a right, and any misuse will result in the withdrawal of that privilege. ICT resources must be properly and efficiently used and are not to be used for any activity relating to fraud, defamation, breach of copyright, unlawful discrimination or vilification, harassment including sexual harassment, stalking, privacy violation, nor any other illegal activity including peer-to-peer file sharing. This is an illustrative but not a comprehensive list.

The Education and Inspections Act 2006 empowers Head teachers to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other e-safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school. Should an incident arise deemed to be of a sufficiently serious nature, it would be at the discretion of the Senior Leadership Team to seek advice of outside agencies, such as the police or the Local authority.

Roles and Responsibilities

The following section outlines the e-safety roles and responsibilities of individuals and groups within the school:

Governors:

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *E-Safety Governor*.

The role of the E-Safety Governor will include:

- regular meetings with the E-Safety Co-ordinator
- regular monitoring of e-safety incident logs
- regular monitoring of filtering
- reporting to relevant Governors

Head teacher and Senior Leaders:

- The Head teacher has a duty of care for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety will be delegated to the E-Safety Co-ordinator.
- The Head teacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.
- The Head teacher / Senior Leaders are responsible for ensuring that the E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their e-safety roles and to train other colleagues, as relevant.
- The Head teacher / Senior Leaders will ensure that there is a robust system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Co-ordinator.

E-Safety Coordinator:

- assumes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.
- liaises with the Local Authority / relevant external body.
- liaises with school technical staff.
- receives reports of e-safety incidents and maintains a log of incidents to inform future e-safety developments.
- meets regularly with the E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs.
- reports regularly to Senior Leadership Team.

Network Manager / Technical staff:

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets required e-safety technical requirements and any Local Authority guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- that the use of the network / internet is regularly monitored in order that any misuse / attempted misuse can be reported to the Head teacher or E-Safety Coordinator (for investigation / action / sanction)

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the Staff Acceptable Use Policy (AUP)
- they report any suspected misuse or problem to the Head teacher / Network Manager / E-Safety Coordinator for investigation / action / sanction

- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- e-safety issues are embedded in all aspects of the curriculum and other activities
- pupils understand and follow the e-safety and acceptable use policies
- pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches
- abide by the Information Sharing Policy and report any data breaches

Child Protection Designated Person:

should be trained in e-safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

- sharing of personal data
- access to illegal / inappropriate materials
- inappropriate on-line contact with adults / strangers
- potential or actual incidents of grooming
- cyber-bullying

Pupils:

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Policy
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.
- should understand the importance of adopting good e-safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

Parents / Carers:

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices / Social media in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- equipment and resources provided by the school
- their children's personal device in the school (where this is allowed)

Community Users / Visitors:

Community Users / Visitors who access school systems / website / VLE as part of the wider school provision will be expected to sign a Community User Acceptable Use Policy before being provided with access to school systems.

Policy Statements

Education –pupils:

Whilst regulation and technical solutions are very important, their use must be balance by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

E-safety should be a focus in all areas of the curriculum and staff should reinforce e-safety messages across the curriculum. The e-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned e-safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key e-safety messages should be reinforced as part of a planned programme of assemblies
- Pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Pupils should be helped to understand the need for the pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies the internet and mobile devices
- in lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

Education – Parents /Carers:

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's on-line behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The school will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. www.swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers

Education & Training – Staff / Volunteers:

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the e-safety training needs of all staff will be carried out regularly.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and Acceptable Use Agreements.
- This E-Safety policy and its updates will be presented to and discussed by staff in staff meetings / INSET days.
- The E-Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors:

Governors should take part in e-safety training / awareness sessions.

This may be offered in a number of ways:

- Attendance at training provided by the Local Authority
- Participation in school training / information sessions for staff or parents.

Technical – infrastructure / equipment, filtering and monitoring:

The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their e-safety responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of school academy technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by Technical support who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password and will be required to change their password regularly.
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the *Head teacher* or other nominated senior leader and kept in a secure place (eg school safe)
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software.

Use of digital and video images:

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use is not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other pupils in the digital / video images.
- Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment, the personal equipment of staff should not be used for such purposes.
- Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website
- Pupil's work can only be published with the permission of the pupil and parents or carers.

Data Protection:

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.
- Explicit consent it received.

The school must ensure that:

- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has a Data Protection Policy
- It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
- Responsible persons are appointed/identified - Senior Information Risk Officer (SIRO) and Information Asset Owners (IAOs)
- Risk assessments are carried out
- It has clear and understood arrangements for the security, storage and transfer of personal data

- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There is a policy for reporting, logging, managing and recovering from information risk incidents
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
- There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner's Office.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device, in line with school policy (below) once it has been transferred or its use is complete

Social Media - Protecting Professional Identity:

Social media (e.g., Facebook, Twitter, Instagram…) is the collective of online communications channels dedicated to community-based input, interaction, content-sharing and collaboration. Social media is becoming an integral part of life online as social websites and applications proliferate. Most traditional online media platforms include social components, such as comment fields for users. However, some online games, for example Minecraft, Roblox, Fortnite, and video sharing platforms such as YouTube, have social media elements to them. All schools, academies and local authorities have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Spring Vale Primary school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through limiting access to personal information:

- Training to include acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk

School staff should ensure that:

- No reference should be made on social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school / academy or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Spring Vale Primary School's use of social media for professional purposes will be checked regularly by the senior risk officer and e-safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Communications:

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x			x				
Use of mobile phones in lessons				x				
Use of mobile phones in social time	x			x				
Taking photos on mobile phones				x				
Use of other mobile devices e.g. tablets, gaming devices	x			x				
Use of personal email addresses in school, or on school network	x			x				
Use of school email for personal emails			x					x
Use of messaging apps	x						x	
Use of social media			x	x				
Use of blogs	x						x	

When using communication technologies Spring Vale Primary school considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored.
- Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and students / pupils or parents / carers (email) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Pupils should be taught about e-safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

- Personal information should not be posted on the school / academy website and only official email addresses should be used to identify members of staff.

Unsuitable / inappropriate activities:

The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school policy restricts usage as follows:

User Actions:		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	pornography				X	
	promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school / academy					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

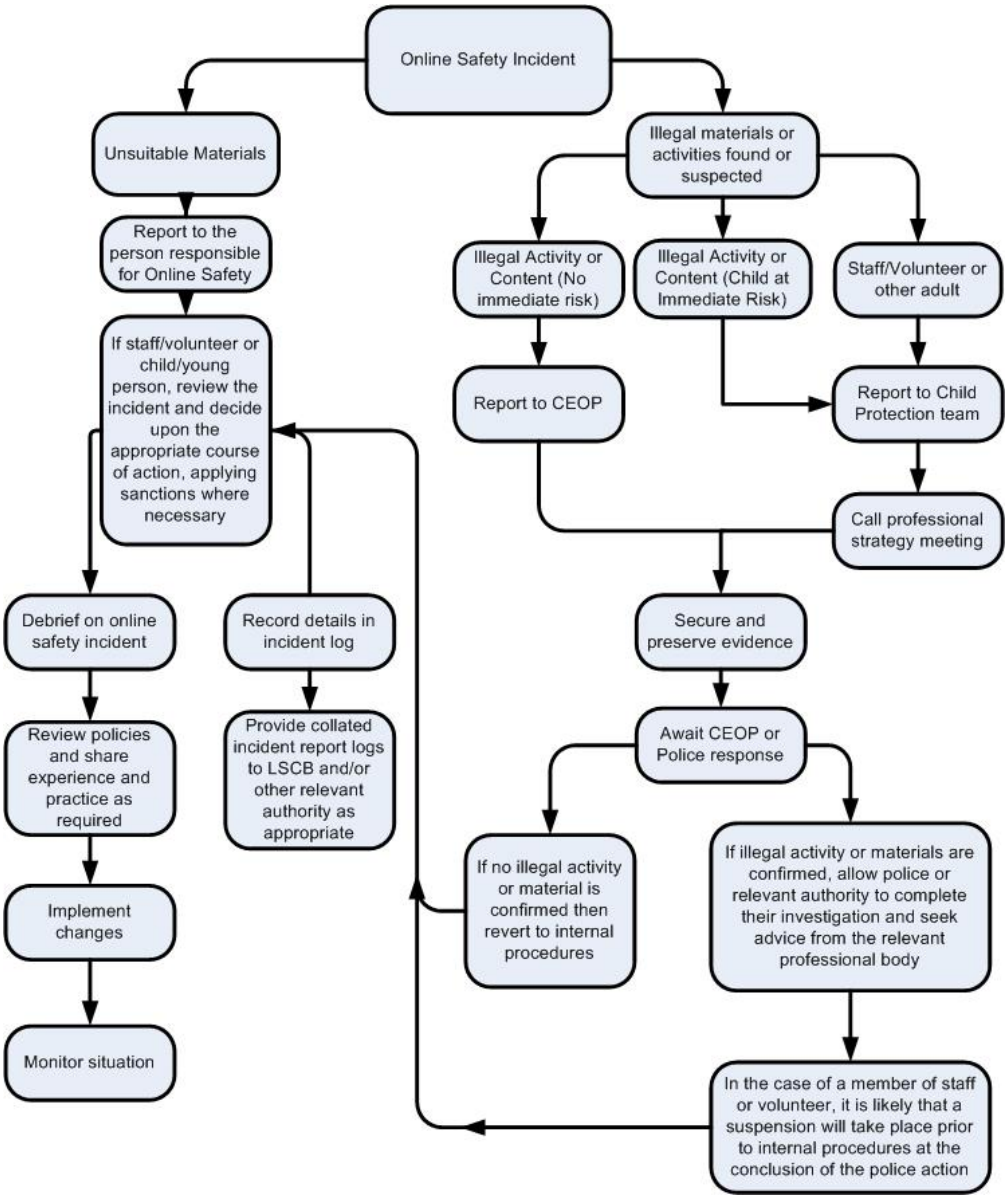
On-line gaming (educational)	X				
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce			X		
File sharing		X			
Use of social media				X	
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube	X				

Responding to incidents of misuse:

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

Illegal Incidents:

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents:

It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)

- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - adult material which potentially breaches the Obscene Publications Act
    - criminally racist material
    - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken, as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions & Sanctions:

It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as follows:

Students / Pupils — Actions / Sanctions

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher / Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X					
Unauthorised use of non-educational sites during lessons					X				
Unauthorised use of mobile phone / digital camera / other mobile device						X			
Unauthorised use of social media / messaging apps / personal email						X			

Unauthorised downloading or uploading of files					X				
Allowing others to access school / academy network by sharing username and passwords					X				
Attempting to access or accessing the school / academy network, using another student's / pupil's account	X								
Attempting to access or accessing the school / academy network, using the account of a member of staff			X						
Corrupting or destroying the data of other users			X						
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature			X						
Continued infringements of the above, following previous warnings or sanctions			X			X			
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school			X						

Security and Privacy:

Security and privacy is important when using computers and devices that connect to the internet. The Spring Vale Primary school Information Sharing Policy outlines the requirements for security and privacy of data. You should ensure you follow the below guidelines to protect the security and privacy of both yourself and others.

- Do not disclose passwords to anyone else. You are responsible for the secrecy of your password and as such you will be responsible for any misuse under your accounts.
- Do not attempt to bypass any security in place on the computers or devices or attempt to alter any settings.
- Downloading and sharing of copyright material can be illegal. Do not download, share or reproduce copyright materials without the express permission of the copyright holder or protection under the 'Fair Use' justification. Acknowledge the source on all resources used.
- You should report the URL/web address of any inappropriate material that is accessed to the technical support team at the earliest opportunity so this can be dealt with.
- Staff should not accept students as 'friends' or contacts within any social networking site. If staff have any students as contacts, they must remove them with immediate effect.
- Staff should maintain a check on the privacy settings of their social media accounts to avoid making their online activity available and accessible to students.

Internet Safety:

- The internet is a privilege and not a right and should only be used for school related activities. The below guidelines should be followed to ensure your access to the internet in schools is not revoked.
- The Internet should only be used for school related activities such as studying, revision or work. Any other activities such as games will result in student accounts being Suspended.

- The Internet should not be used to download, print or obtain unlawful, obscene or abusive materials. Students should also be cautious when downloading files such as documents and PDFs from the Internet as they may contain viruses.
- The Internet should not be used for engaging in chat activities. Any such activity will result in student accounts being banned.
- Internet access is filtered in school using software to restrict access to inappropriate material. Any material that is found and considered to be inappropriate should be immediately reported to the technical support team to be dealt with accordingly.
- Students must disclose to their teacher or other staff member any message or other activity online they receive that is considered inappropriate, offensive or makes them feel uncomfortable so this can be dealt with in a timely manner.
- The Internet should not be used to access indecent, unlawful, pornographic or otherwise offensive material. Any person found doing so will immediately be removed from the school network and any computer and Internet privileges will be revoked indefinitely.

Preventing Extremism and Radicalisation:

Spring Vale Primary school is committed to providing a secure environment for all of its students, staff and visitors. The current threat from terrorism extremism in the United Kingdom can involve the exploitation of vulnerable people, including children, young people and vulnerable adults to involve them in terrorism or activity in support of terrorism. Spring Vale values freedom of speech and the expression of beliefs / ideology as fundamental rights underpinning our society's values. Both students and teachers have the right to speak freely and voice their opinions.

However, freedom comes with responsibility and free speech that is designed to manipulate the vulnerable or that leads to violence or harm of others goes against the moral principles in which freedom of speech is valued. Free speech is not an unqualified privilege; it is subject to laws and policies governing equality, human rights, community safety and community cohesion.

The current threat from terrorism in the United Kingdom may include the exploitation of vulnerable people, to involve them in terrorism or in activity in support of extremism and terrorism. The normalisation of extreme views may also make children and young people vulnerable to future manipulation and exploitation.

Spring Vale Primary school is clear that this exploitation and radicalisation should be viewed as a safeguarding concern. Any concerns relating to e-safety or safeguarding should be reported to a member of the safeguarding team. In adherence to this policy, and the procedures therein, staff, governors, volunteers and visitors will contribute to Spring Vale Primary school's delivery of the outcomes to all children, as set out in the Children Act 2004.

School Ethos and Practice:

There is no place for extremist views of any kind in our schools, whether from internal sources – students, staff or governors, or external sources - school community, external agencies or individuals. It is imperative that our students and parents see our school as a safe place where they can discuss and explore controversial issues safely and in an unbiased way and where our teachers encourage and facilitate this.
As a school we recognise that extremism and exposure to extremist materials and influences can lead to poor outcomes for our students. We also recognise that if we fail to challenge extremist views we are failing to protect our students.

Extremists of all persuasions aim to develop destructive relationships between different communities by promoting division, fear and mistrust of others based on ignorance or prejudice and thereby limiting the life chances of young people. Education is a powerful weapon against this; equipping young people with the knowledge, skills and critical thinking, to challenge and debate in an informed way.

Therefore, Spring Vale will provide a broad and balanced curriculum, delivered by skilled professionals, so that our pupils are enriched, understand and become tolerant of difference and diversity and also to ensure that they thrive, feel valued and not marginalised.

We are aware that young people can be exposed to extremist influences or prejudiced views from an early age which emanate from a variety of sources and media, including via the internet, and at times students may themselves reflect or display views that may be discriminatory, prejudiced or extremist, including using derogatory language.

Any prejudice, discrimination or extremist views, including derogatory language, displayed by students, staff, visitors or parents will always be challenged and where appropriate dealt with. Where misconduct by a teacher is proven the matter will be referred to the National College for Teaching and Leadership for their consideration as to whether to a Prohibition Order is warranted.
As part of wider safeguarding responsibilities school staff will be alert to:

- Disclosures by students of their exposure to the extremist actions, views or materials of others outside of school, such as in their homes or community groups, especially where students have not actively sought these out.
- Graffiti symbols, writing or art work promoting extremist messages or images
- Students accessing extremist material online, including through social networking sites
- Parental reports of changes in behaviour, friendship or actions and requests for assistance
- Local schools, Local Authority services, and police reports of issues affecting pupils in other schools or settings
- Students voicing opinions drawn from extremist ideologies and narratives
- Use of extremist or 'hate' terms to exclude others or incite violence
- Intolerance of difference, whether secular or religious or, in line with our equalities policy, views based on, but not exclusive to, gender, disability, homophobia, race, colour or culture
- Attempts to impose extremist views or practices on others
- Anti-Western or Anti-British views

Filtering and Monitoring:

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for e-safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school. All devices on the school network are connected to our filtering system, and this is also pushed out to all student, staff and visitor personal devices before they can access the internet. The filtering system has some flexibility at local level, to which the school can use to meet the learning needs of students. These changes have to be approved by the Network Manager or members of the ICT Technical support team.

Spring Vale Primary school e-safety trained staff will consider carefully the issues raised and decide:

- Whether they will use the provided filtering service without change or to allow flexibility for sites to be added or removed from the filtering list for their organisation.
- Whether to introduce differentiated filtering for different groups / ages of users
- Whether to remove filtering controls for some internet use (e.g. social networking sites) at certain times of the day or for certain users.
- Who has responsibility for such decisions and the checks and balances put in place
- What other system and user monitoring systems will be used to supplement the filtering system and how these will be used.

Monitoring:

Spring Vale Primary school uses Meraki Monitoring Software and will therefore monitor the activities of users on the school network and on school equipment as indicated in the School E-Safety Policy and the Acceptable Use Agreement. All staff should be aware of the use of the monitoring software, and ongoing support will be provided by the Technical Support Team.